Jan Krhovják

Fakulta informatiky

Masarykova univerzita

Botanická 68a, 602 00 Brno

POSUDEK DIPLOMOVÉ PRÁCE

Datum: 20.1.2013

Student: Bc. Jakub Skalický

Vedoucí DP: Mgr. et Mgr. Jan Krhovják, Ph.D.

Oponent DP: prof. RNDr. Aleš Drápal, CSc., DSc.

Název: Efektivní aritmetika eliptických křivek nad konečnými tělesy

Zpráva:

Úvodem tohoto posudku bych rád poznamenal, že jakožto formální vedoucí práce (hlavním konzultantem byl Dr. Paul C. Leyland) jsem se k práci během jejího vytváření dostával až v posledních měsících před jejím prvním odevzdáním. První ucelené verze textu také vznikly až na přelomu dubna/května 2012. S obsahem práce jsem i přesto po několika pročteních dobře obeznámen. Pro účely objektivního posouzení práce však poznamenávám, že detailní posouzení některých techničtějších důkazů stejně jako posouzení množství obsahu práce, které musel student nově nastudovat (ve srovnání s látkou standardně přednášenou na MFF UK), ponechávám plně v kompetenci oponenta práce.

Student se v diplomové práci zabývá efektivní aritmetikou eliptických křivek nad konečnými tělesy. První kapitola práce je věnována definicím základních algebraických pojmů vedoucích až k definici eliptických křivek. V samotném závěru kapitoly se student také (okrajově) dostává k aplikaci eliptických křivek v kryptografii a k případným dopadům použitých (konečných) těles na rychlost aritmetiky s eliptickými křivkami. V druhé kapitole je popsán přechod od afinních k projektivním souřadnicím – student zde demonstruje dopad takovýchto reprezentací bodů na rychlost základních operací s nimi. Závěrečné kapitoly práce jsou zaměřeny na Edwardsovy křivky (obecné a binární). Student zde nejprve dokazuje, že obecné Edwarsovy křivky jsou Eliptickými křivkami, a následně se zaměřuje na dokázání tvrzení (a odvození algoritmu) převodu Weierstrassových křivek na Edwardsovy křivky (a naopak). Pozornost je věnována také efektivitě základních operací s body na Edwardsových křivkách.

Oproti původní verzi práce prošla první kapitola na mnohých místech drobnými revizemi – byla reformulována některá tvrzení a odstraněny oponentem vytýkané nejednoznačnosti a chyby ve formalizmech. Druhá kapitola zaznamenala spíše jen syntaktické změny v zápisech algoritmů. Nejvíce práce student věnoval vylepšení částí pojednávajících o nebinárních Edwardsových křivkách, kde byla změněna logika celého dokazování (vycházející z definice obecných Edwardsowých křivek) a došlo k přidání dokázání tvrzení (a odvození algoritmu) převodu Weierstrassových křivek na Edwardsovy křivky (a naopak). Další části práce již příliš mnoho zásadních změn nepřinášejí. Některé připomínky z předcházejících posudků zůstaly i v této verzi práce nepovšimnuty (zejména problém diskrétního logaritmu, navrhované obohacení druhé kapitoly, ale i drobnosti typu „cache“ atp.).

Celkově je text dobře strukturován a jednotlivé kapitoly jsou dobře provázány. Přínosem diplomanta je v práci zejména shromáždění poznatků o tématu z různých zdrojů a vzájemné srovnání efektivity jednotlivých algoritmů pro různé reprezentace křivek. K práci s odbornou literaturou nemám výhrad. Po typografické stránce je práce na výborné úrovni. Po gramatické stránce jsem v práci nalezl poměrně dosti triviálních překlepů (např. coefficents, elliminate, occurence, expceptional, neccessity, additionaly, higly, trasformation, sotfware), které student mohl snadno a rychle dohledat a odstranit současnými nástroji pro kontrolu pravopisu/gramatiky.

Hodnocení:

Předloženou práci i přes výše uvedené výtky doporučuji uznat jako diplomovou a v případě dobré obhajoby navrhuji hodnocení stupněm **velmi dobře**.

Jan Krhovják